

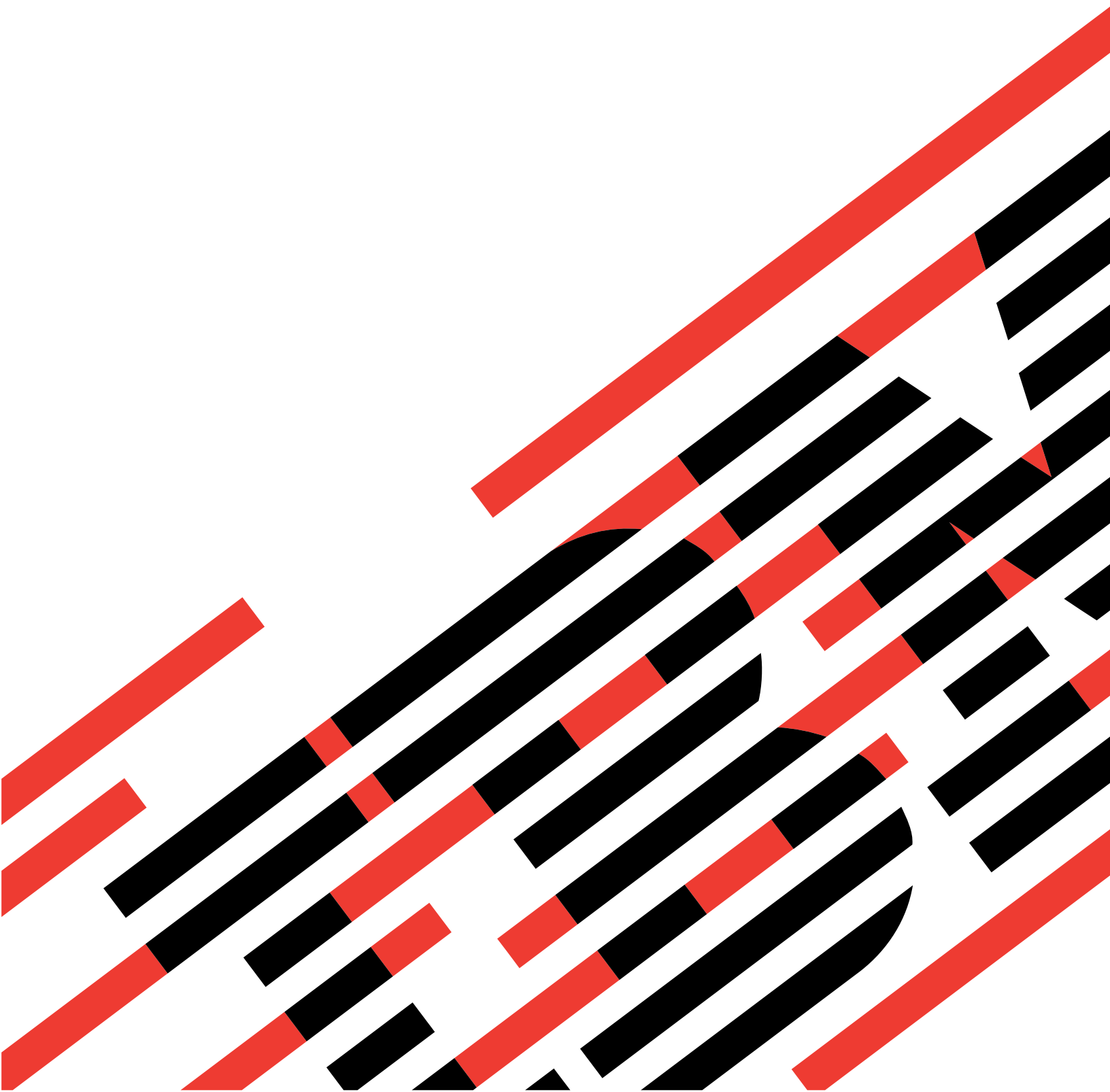
IBM

@server

iSeries

Secure Sockets Layer (SSL)

バージョン 5 リリース 3





@server

iSeries

Secure Sockets Layer (SSL)

バージョン 5 リリース 3

お願い

本書および本書で紹介する製品をご使用になる前に、23 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM OS/400 (プログラム番号 5722-SS1) バージョン 5、リリース 3、モディフィケーション 0 に適用されます。また、改訂版で断りがない限り、それ以降のすべてのリリースおよびモディフィケーションにも適用されます。このバージョンは、すべての RISC モデルで稼動するとは限りません。また CISC モデルでは稼動しません。

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

<http://www.ibm.com/jp/manuals/main/mail.html>

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

<http://www.ibm.com/jp/manuals/> の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原 典： iSeries
Secure Sockets Layer (SSL)
Version 5 Release 3

発 行： 日本アイ・ピー・エム株式会社

担 当： ナショナル・ランゲージ・サポート

第1刷 2005.8

この文書では、平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財)日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、
平成角ゴシック体™W5、平成角ゴシック体™W7

© Copyright International Business Machines Corporation 2002, 2005. All rights reserved.

© Copyright IBM Japan 2005

目次

Secure Sockets Layer (SSL)	1	サーバー認証	17
V5R3 の新機能	1	クライアント認証	18
トピックの印刷	2	SSL を使用可能にする計画	18
シナリオ	2	SSL によるアプリケーションの保護	19
シナリオ: SSL によるマネージメント・セントラル・サーバーへのクライアント接続の保護	3	SSL のトラブルシューティング	19
シナリオ: SSL によるマネージメント・セントラル・サーバーへのすべての接続の保護	6	関連情報	20
概念	15	付録. 特記事項.	23
SSL の歴史	15	商標	24
SSL の仕組み	15	資料に関するご使用条件	24
サポートされている SSL および Transport Layer Security (TLS) プロトコル	16		

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) は、非保護ネットワーク (インターネットなど) を介して、アプリケーションでセキュアな通信セッションを行えるようにするための業界標準になっています。SSL および iSeries™ サーバー・アプリケーションに関する詳細は、以下のリンクを参照してください。

- **V5R3 の新機能**
SSL に関する新機能または利用できる新しい情報について説明します。
- **SSL シナリオ**
SSL の情報に新しく追加されたものであり、SSL がどのように機能するか実現可能な例を挙げることで、iSeries サーバーでの SSL の実行に関する理解を深める目的があります。
- **SSL の概念**
補足情報であり、Secure Sockets Layer (SSL) プロトコルを構成する基本的な要素を説明します。
- **SSL を使用可能にする計画**
iSeries サーバーで SSL を使用可能にするための前提条件、および役に立つヒントが記載されています。
- **SSL によるアプリケーションの保護**
iSeries サーバーで SSL を使用してセキュアにできるアプリケーションのリストが記載されています。
- **SSL のトラブルシューティング**
iSeries サーバーで行う SSL のトラブルシューティングの処置を開始する方法の基本的な手引きです。
- **関連情報**
追加の情報源へのリンクが記載されています。

V5R3 の新機能


今回のリリースでは、Secure Sockets Layer (SSL) に関して注目すべき 2 つの新しい項目があります。

1. シナリオ: SSL によるマネージメント・セントラル・サーバーへのクライアント接続の保護

これは、SSL を使用して、リモート・クライアントと iSeries サーバーのマネージメント・セントラル・サーバーとの接続を保護する方法を説明した新しいシナリオです。iSeries サーバーは、ローカル・エリア・ネットワーク (LAN) のセントラル・システムに指定されています。



2. GSKit API の GSKit バージョン 6B

V5R3 より、GSKit API は GSKit のバージョン 6B を基にしています。旧リリースでは、GSKit のバージョン 4D を基にしていました。GSKit API についての詳細は、こちらをクリックしてください。

今回のリリースでの新機能や変更された機能に関する詳細は、「iSeries プログラム資料説明書」 を参照してください。

新規箇所または変更箇所を見つける方法

技術上の変更点を見つけるには、次の記号を使用します。

-  記号は、新規の情報または変更された情報の開始点を示します。
-  記号は、新規の情報または変更された情報の終了点を示します。

トピックの印刷

この文書の PDF 版を参照用または印刷用にダウンロードし、表示することができます。実行するには、「Secure Sockets Layer (SSL)」(約 412 KB) を選択します。

その他の情報

このトピックについての関連情報も表示したり、印刷することができます。

PDF ファイルの保存

表示用または印刷用の PDF ファイルをワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を右クリックする。
2. 「リンクを名前を付けて保存」(Netscape Navigator) または「対象をファイルに保存」(Internet Explorer) をクリックする。
3. PDF を保存したいディレクトリーに進む。
4. 「保存」をクリックする。

Adobe Acrobat Reader のダウンロード

これらの PDF を表示または印刷するには、Adobe Acrobat Reader が必要です。これは、Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html)  から、ダウンロードできます。

シナリオ

以下のシナリオは、iSeries サーバーで SSL を使用可能にするための利点を、最大限に活用することを目的としています。

- シナリオ: SSL によるマネージメント・セントラル・サーバーへのクライアント接続の保護

このシナリオは、SSL を使用して、リモート・クライアントと iSeries サーバーとの接続を保護する方法を説明しています。iSeries サーバーは、iSeries ナビゲーターのマネージメント・セントラル・サーバーを使用して、セントラル・システムとして機能しています。

- シナリオ: SSL によるマネージメント・セントラル・サーバーへのすべての接続の保護

このシナリオは、SSL を使用して、iSeries サーバーとのすべての接続を保護する方法を説明しています。iSeries サーバーは、iSeries ナビゲーターのマネージメント・セントラル・サーバーを使用して、セントラル・サーバーとして機能しています。

- シナリオ: SSL による FTP の保護

このシナリオは、FTP アプリケーションで SSL を使用可能にする方法を説明しています。

- シナリオ: SSL による Telnet の保護

このシナリオは、Telnet アプリケーションで SSL を使用可能にする方法を説明しています。

- シナリオ: iSeries での SSL のパフォーマンスの改善

このシナリオは、iSeries サーバーで SSL のパフォーマンスを改善するために、暗号化ハードウェアを使用する方法を説明しています。

- シナリオ: 暗号化ハードウェアによる秘密鍵の保護

このシナリオは、iSeries サーバーでの SSL トランザクションに関連した秘密鍵を保護するために、暗号化ハードウェアを使用する方法を説明しています。

シナリオ: SSL によるマネージメント・セントラル・サーバーへのクライアント接続の保護



状況

ある企業が、オフィスに iSeries サーバーを数台組み込んだローカル・エリア・ネットワーク (LAN) を構築しています。この企業のシステム管理者であるボブは、この iSeries サーバーの 1 つを LAN のセントラル・システム (今後、システム A と呼びます) に指定しました。ボブは、システム A でマネージメント・セントラル・サーバーを使用して、LAN 上にある他のエンドポイントをすべてを管理しています。

ボブは、システム A のマネージメント・セントラル・サーバーに、社内 LAN の外部のネットワークから接続されることを心配しています。ボブは出張が多いため、外出している間、マネージメント・セントラル・サーバーへのセキュアな接続が必要です。彼はオフィスにいない場合、自分の PC とマネージメント・セントラル・サーバーの間の接続を確実にセキュアにしたいと思っています。ボブは、自分の PC とシステム A のマネージメント・セントラル・サーバーで、SSL を使用可能にすることを決めました。このように SSL を使用可能にすると、出張時にマネージメント・セントラル・サーバーへの接続を確実にセキュアにすることができます。

目的

ボブは、自分の PC とマネージメント・セントラル・サーバーの間の接続を確実にセキュアにしたいと思っています。ボブは、システム A 上のマネージメント・セントラル・サーバーと LAN 上のエンドポイントの間の接続に、セキュリティーを追加する必要は感じていません。この企業のオフィスで働いている他の従業員たちも、マネージメント・セントラル・サーバーへの接続に関して、追加のセキュリティーを必要としていません。ボブの計画は、クライアント接続でサーバー認証を使用するように、自分の PC とシステム A のマネージメント・セントラル・サーバーを構成することです。他の PC または LAN 上の iSeries サーバーからマネージメント・セントラル・サーバーへの接続は、SSL により保護されていません。

詳細

次の表は、PC クライアント上で SSL が使用可能であるか使用不可であるかに基づき、使われる認証のタイプを説明したものです。

表 1. SSL によるクライアントとマネージメント・セントラル・サーバー間の接続の保護に必要な要素

ボブの PC での SSL の状況	システム A のマネージメント・セントラル・サーバーに指定された認証レベル	SSL 接続が使用可能か
SSL 設定はオフ	任意	いいえ
SSL 設定はオン	任意	はい (サーバー認証)

サーバー認証は、ボブの PC でマネージメント・セントラル・サーバーの証明書を認証することを意味します。マネージメント・セントラル・サーバーに接続する場合は、ボブの PC は SSL クライアントとして機能します。マネージメント・セントラル・サーバーは、SSL サーバーとして機能し、ID を証明しなければなりません。マネージメント・セントラル・サーバーは、ボブの PC が信頼する認証局 (CA) により発行された証明書を提供することによって、ID を証明します。

前提条件および前提事項

ボブは、自分の PC とシステム A のマネージメント・セントラル・サーバーの間の接続を保護するため、以下の管理タスクおよび構成タスクを行わなければなりません。

1. システム A を SSL の前提条件 (『SSL の前提条件』を参照) に合わせる。
2. OS/400® の V5R3 (またはそれ以上のバージョン) をシステム A にインストールする。システム A が OS/400 の V5R1 で稼動している場合、以下の OS/400 (5722-SS1) 用のフィックス (PTF) をインストールします。
 - a. SI01375
 - b. SI01376
 - c. SI01377
 - d. SI01378
 - e. SI01838
3. iSeries ナビゲーター PC クライアントが iSeries Access for Windows® の V5R3 以降を実行する。
4. iSeries サーバーの認証局 (CA) を取得する。
5. システム A 用に CA によって署名された証明書を作成する。
6. CA および証明書をシステム A に送信し、それらを鍵データベースにインポートする。
7. マネージメント・セントラル・サーバーの ID を証明書に割り当てる。
 - a. システム A で、IBM® デジタル証明書マネージャーを始動する。ボブが証明書の取得または作成を行います。もしくは、ここで認証システムのセットアップまたは変更を行います。認証システムをセットアップする方法については、『デジタル証明書マネージャーの使用』を参照してください。
 - b. 「証明書ストアの選択 (Select a Certificate Store)」を選択します。
 - c. 「*SYSTEM」を選択し、「続行」をクリックします。
 - d. 「証明書ストア・パスワード (Certificate Store password)」に *SYSTEM を入力し、「続行」をクリックします。メニューが再ロードされたら、「アプリケーションの管理 (Manage Applications)」を展開します。
 - e. 「証明書割り当ての更新 (Update certificate assignment)」をクリックします。
 - f. 「サーバー」を選択し、「続行」をクリックします。
 - g. 「マネージメント・セントラル・サーバー (Management Central Server)」を選択し、「証明書割り当ての更新 (Update certificate assignment)」をクリックします。これによって、iSeries Access for Windows クライアントに対して ID (サーバーの識別) の確立に使用する証明書を、マネージメント・セントラル・サーバーに割り当てます。
 - h. 「新しい証明書の割り当て (Assign New Certificate)」をクリックします。DCM は、「証明書割り当ての更新 (Update certificate assignment)」ページを再ロードして、確認メッセージを表示します。
 - i. 「終了 (Done)」をクリックします。
8. iSeries ナビゲーターをセットアップする。
 - a. PC クライアントで iSeries ナビゲーターの SSL コンポーネントを選択してインストールします。
 - b. CA を PC のクライアントにダウンロードします。

構成ステップ

ボブは、SSL によって、自分の PC からシステム A のマネージメント・セントラル・サーバーへの接続を保護するために、次のステップを完了する必要があります。

1. ステップ 1: iSeries ナビゲーター・クライアントについて SSL を非アクティブにする
2. ステップ 2: マネージメント・セントラル・サーバーの認証レベルを設定する
3. ステップ 3: システム A のマネージメント・セントラル・サーバーを再始動する
4. ステップ 4: iSeries ナビゲーター・クライアントについて SSL をアクティブにする
5. オプション・ステップ: iSeries ナビゲーター・クライアントについて SSL を非アクティブにする

拡張した構成ステップを表示するには、『SSL によるマネージメント・セントラル・サーバーへのクライアント接続の保護』を参照してください。

構成の詳細: SSL によるマネージメント・セントラル・サーバーへのクライアント接続の保護

次の情報は、『シナリオ: SSL によるマネージメント・セントラル・サーバーへのクライアント接続の保護』に目を通していることを前提としています。このシナリオでは、iSeries サーバーは、企業のローカル・エリア・ネットワーク (LAN) のセントラル・システムに指定されています。ボブは、セントラル・システム (ここではシステム A と呼びます) 上のマネージメント・セントラル・サーバーを使用して、企業のネットワークのエンドポイントを管理しています。次の情報で、マネージメント・セントラル・サーバーに対する外部のクライアント接続を保護するために必要なステップを行う方法を説明します。ボブがシナリオの構成ステップを完了するのを追っていきます。

ボブがマネージメント・セントラル・サーバーで SSL を使用可能にするためには、まずその前に前提条件のプログラムをインストールし、iSeries サーバーにデジタル証明書をセットアップする必要があります。続ける前に、このシナリオに関して『前提条件および前提事項』を参照してください。前提条件を満たしたら、以下の手順を完了させて、マネージメント・セントラル・サーバーで SSL を使用可能にできます。

ステップ 1: iSeries ナビゲーター・クライアントについて SSL を非アクティブにする。

1. iSeries ナビゲーターで、「ユーザー接続」を展開します。
2. システム A を右クリックし、「プロパティ」を選択します。
3. 「セキュア・ソケット (Secure Sockets)」タブをクリックし、「接続に Secure Sockets Layer (SSL) を使用する (Use Secure Sockets Layer (SSL) for connection)」を選択解除します。
4. iSeries ナビゲーターを終了し、再始動します。

パッドロックが、iSeries ナビゲーターのマネージメント・セントラル・コンテナーから見えなくなります。これは、接続が非セキュアであるということを示しています。このことは、ボブが、クライアントと企業のセントラル・システムの間で SSL で保護された接続を保持していないことを示しています。

ステップ 2: マネージメント・セントラル・サーバーの認証レベルを設定する。

1. iSeries ナビゲーターで、「マネージメント・セントラル」を右クリックし、「プロパティ」を選択します。
2. 「セキュリティー (Security)」タブをクリックし、「Secure Sockets Layer (SSL) を使用する (Use Secure Sockets Layer (SSL))」を選択します。
3. 認証レベルでいずれかを選択します。(V5R3 以降の iSeries Access for Windows で使用可能です。)
4. 「OK」をクリックして、この値をセントラル・システムに設定します。

ステップ 3: セントラル・システム上のマネージメント・セントラル・サーバーを再始動する

1. iSeries ナビゲーターで、「ユーザー接続」を展開します。

2. 「システム A」で「ネットワーク」->「サーバー」の順に展開し、「TCP/IP」を選択します。
3. 「マネージメント・セントラル」を右クリックし、「停止」を選択します。「セントラル・システム (central system)」ビューは縮小表示され、サーバーには接続されていないという内容のメッセージが表示されます。
4. マネージメント・セントラル・サーバーが停止したら、「開始」をクリックして、再始動します。

ステップ 4: iSeries ナビゲーター・クライアントについて SSL をアクティブにする

1. iSeries ナビゲーターで、「ユーザー接続」を展開します。
2. システム A を右クリックし、「プロパティ」を選択します。
3. 「セキュア・ソケット (Secure Sockets)」タブをクリックし、「接続に Secure Sockets Layer (SSL) を使用する (Use Secure Sockets Layer (SSL) for connection)」を選択します。
4. iSeries ナビゲーターを終了し、再始動します。

パッドロックは、iSeries ナビゲーターのマネージメント・セントラル・サーバーの横に表示されます。これは、SSL で接続がセキュアになっていることを示します。このことは、ボブが、彼のクライアントと彼の企業のセントラル・システムの間で SSL でのセキュアな接続をアクティブにするのに成功したということを示しています。

注: この手順は、1 つの PC とマネージメント・セントラル・サーバーの間の接続のみをセキュアにします。マネージメント・セントラル・サーバーへの他のクライアント接続や、エンドポイントからマネージメント・セントラル・サーバーへの接続は、セキュアになりません。他のクライアントをセキュアにするためには、前提条件を満たしていることを確認してから、『ステップ 4』を繰り返し行ってください。マネージメント・セントラル・サーバーとの他の接続をセキュアにするには、『シナリオ: SSL によるマネージメント・セントラル・サーバーへのすべての接続の保護』を参照してください。

オプション・ステップ: iSeries ナビゲーター・クライアントについて SSL を非アクティブにする

ボブがオフィスで仕事をしていて、SSL 接続によって彼の PC のパフォーマンスに影響を与えたくない場合は、次のステップを実行することで簡単に SSL を非アクティブにすることができます。

1. iSeries ナビゲーターで、「ユーザー接続」を展開します。
2. 「マネージメント・セントラル」を右クリックし、「プロパティ」を選択します。
3. 「セキュア・ソケット (Secure Sockets)」タブをクリックし、「接続に Secure Sockets Layer (SSL) を使用する (Use Secure Sockets Layer (SSL) for connection)」を選択解除します。
4. iSeries ナビゲーターを終了し、再始動します。

パッドロックは、iSeries ナビゲーターのマネージメント・セントラル・サーバーから見えなくなります。これは、接続が非セキュアであることを示しています。このことは、ボブが、彼の PC クライアントとシステム A のマネージメント・セントラル・サーバーの間に、SSL で保護された接続を保持していないことを示しています。

他の SSL のシナリオのリンクに関しては、『シナリオ』を参照してください。

シナリオ: SSL によるマネージメント・セントラル・サーバーへのすべての接続の保護

状況

ある企業が最近、iSeries サーバーをリモート・ロケーション (エンドポイント) に置く広域ネットワークをセットアップしました。エンドポイントは、メイン・オフィスにある 1 台の iSeries サーバー (セントラ

ル・システム) によって中央管理されています。トムは、この企業のセキュリティー・スペシャリストです。トムは、企業のセントラル・システムのマネージメント・セントラル・サーバーと、すべてのエンドポイント・サーバーおよびクライアントとの間の接続を、すべてセキュアにするために、Secure Sockets Layer (SSL) を使用したいと思っています。

詳細

トムは、SSL を使用することにより、マネージメント・セントラル・サーバーへのすべての接続を、セキュアに管理することができます。マネージメント・セントラル・サーバーで SSL を使用するには、トムは、セントラル・システムにアクセスに使用する PC で、iSeries Access for Windows および iSeries ナビゲーターをセキュアにしなければなりません。

次の 2 つから認証レベルを選択します。

サーバー認証

エンドポイント・システム・サーバー証明書の認証を行います。エンドポイント・システムに接続する場合は、セントラル・システムは SSL クライアントとして機能します。エンドポイント・システムは SSL サーバーとして機能し、セントラル・システムが信頼する認証局によって発行された証明書を提供することによって、ID を証明しなければなりません。すべてのエンドポイント・システムには、トラステッド CA から有効な証明書が発行される必要があります。

クライアントおよびサーバー認証

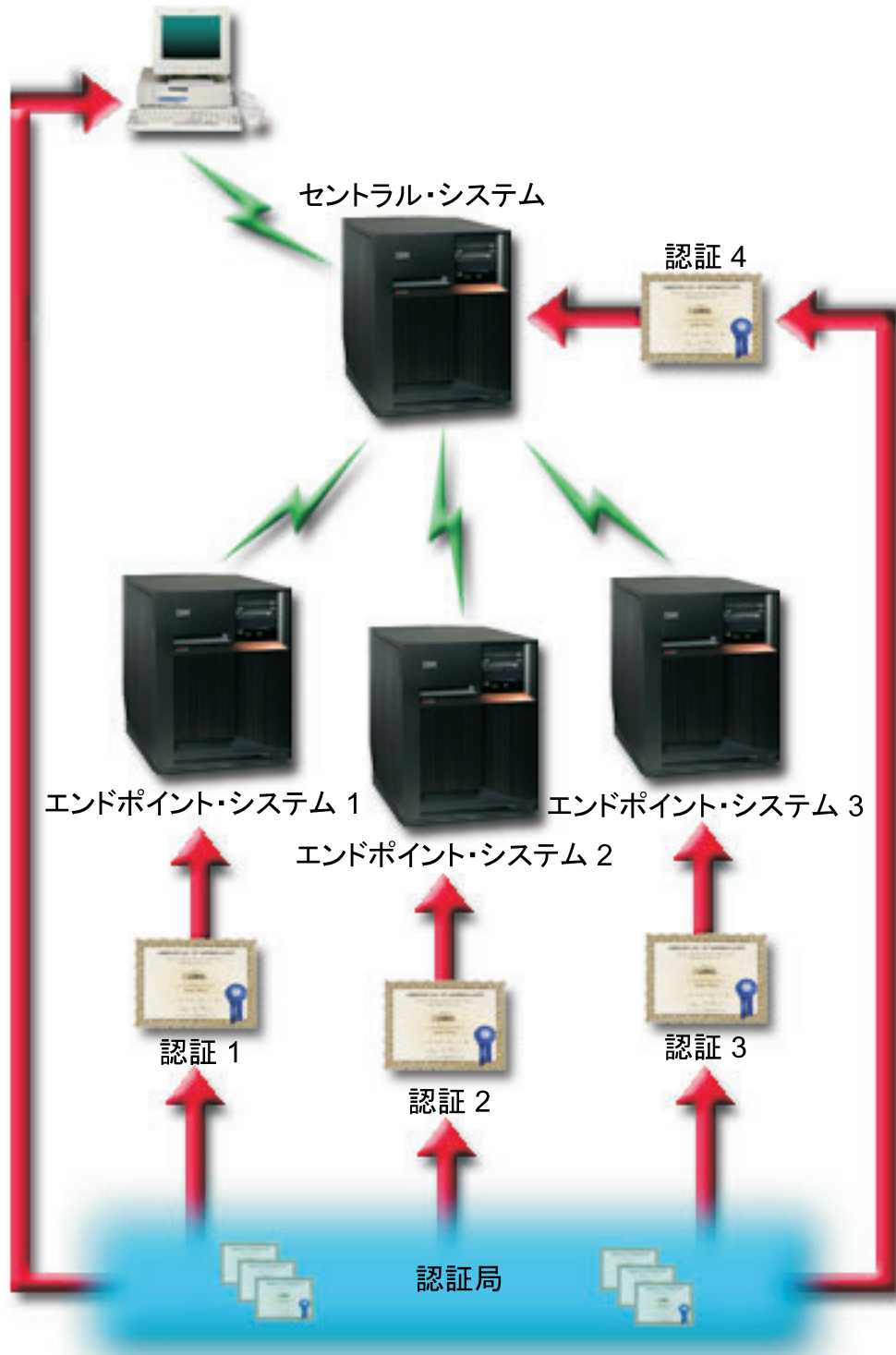
セントラル・システム証明書とエンドポイント・システム証明書の両方の認証を行います。この認証は、サーバー認証レベルよりも高いセキュリティー・レベルです。他のアプリケーションでは、この認証はクライアント認証と呼ばれています。その場合、クライアントは有効な信頼できる証明書を提供する必要があります。セントラル・システム (SSL クライアント) がエンドポイント・システム (SSL サーバー) との接続を確立しようとする時、セントラル・システムとエンドポイント・システムは、互いの証明書の CA 認証性を認証します。

他のアプリケーションと異なり、マネージメント・セントラルは、トラステッド・グループ妥当性検査リストと呼ばれる妥当性検査リストを通して認証を提供します。一般に、妥当性検査リストには、ユーザーを識別する情報 (たとえば、ユーザー ID) と認証情報 (たとえば、パスワード、個人識別番号、デジタル証明書) が保管されています。この認証情報は暗号化されています。

大半のアプリケーションでは通常、サーバー認証とクライアント認証の両方を使用可能にすることを指定しません。これは、サーバー認証が、ほとんど常に SSL セッションが使用可能になっている間に発生するためです。多くのアプリケーションには、クライアント認証の構成のオプションがあります。セントラル・システムがネットワークで果たす役割は 2 つあるので、マネージメント・セントラルでは、クライアント認証ではなく、「サーバーおよびクライアント認証」という用語を使用しています。PC ユーザーがセントラル・システムに接続し、SSL が使用可能になっている場合は、セントラル・システムはサーバーとして機能します。しかし、セントラル・システムがエンドポイント・システムに接続する場合、セントラル・システムはクライアントとして機能します。次の図は、セントラル・システムがネットワークでサーバーおよびクライアントとして機能する様子を示したものです。

注: この図では、認証局に関連付けられた証明書は、セントラル・システム、およびすべてのエンドポイント・システム上の鍵データベースに保管する必要があります。

iSeries ナビゲーター・クライアント



前提条件および前提事項

トムは、マネージメント・セントラル・サーバーへのすべての接続を保護するために、以下の管理タスクおよび構成タスク (SSL によってセキュアになっているマネージメント・セントラルの広域ネットワーク (WAN) の図を参照) を行う必要があります。

1. セントラル・システムを SSL の前提条件 (『SSL の前提条件』を参照) に合わせる。
2. セントラル・システムおよびすべてのエンドポイントの iSeries サーバーを OS/400 の V5R2 以降で稼動する。セントラル・システムおよびエンドポイントが OS/400 の V5R1 で稼動している場合、以下の OS/400 (5722-SS1) 用のフィックス (PTF) をインストールします。
 - a. SI01375
 - b. SI01376
 - c. SI01377
 - d. SI01378
 - e. SI01838
3. iSeries ナビゲーター PC クライアントが iSeries Access for Windows の V5R2 以降を実行する。クライアントが V5R1 である場合、サービス・パック PTF SI01907 (以降) を V5R1 の iSeries Access for Windows (5722-XE1) にインストールします。
4. iSeries サーバーの認証局 (CA) を取得する。
5. SSL が使用可能になっているマネージメント・セントラル・サーバーが管理する iSeries サーバーごとに、CA で署名された証明書を作成する。
6. CA および証明書をそれぞれの iSeries サーバーに送信し、それらを鍵データベースにインポートする。
7. マネージメント・セントラルのアプリケーション ID および iSeries ナビゲーターが使用するすべてのエンドポイント・サーバーのアプリケーション ID が記載されている証明書を割り当てる。
 - a. セントラル・サーバーで IBM デジタル証明書マネージャーを開始します。トムが証明書を取得または作成する必要がある場合、あるいは証明書システムをセットアップまたは変更する必要がある場合には、それをこの時点で行います (証明書システムのセットアップの詳細は、『デジタル証明書マネージャーの使用』を参照)。
 - b. 「証明書ストアの選択 (Select a Certificate Store)」を選択します。
 - c. 「*SYSTEM」を選択し、「続行」をクリックします。
 - d. 「証明書ストア・パスワード (Certificate Store password)」に *SYSTEM を入力し、「続行」をクリックします。メニューが再ロードされたら、「アプリケーションの管理 (Manage Applications)」を展開します。
 - e. 「証明書割り当ての更新 (Update certificate assignment)」をクリックします。
 - f. 「サーバー」を選択し、「続行」をクリックします。
 - g. 「マネージメント・セントラル・サーバー (Management Central Server)」を選択し、「証明書割り当ての更新 (Update certificate assignment)」をクリックします。これにより、証明書が使用するマネージメント・セントラル・サーバーに割り当てられます。
 - h. 「新しい証明書の割り当て (Assign New Certificate)」をクリックします。DCM は、「証明書割り当ての更新 (Update certificate assignment)」ページを再ロードして、確認メッセージを表示します。
 - i. 「終了 (Done)」をクリックします。
 - j. iSeries ナビゲーターが使用するすべてのエンドポイント・サーバーについて、この手順を繰り返します。
8. iSeries ナビゲーターをセットアップする。

- a. PC クライアントで iSeries ナビゲーターの SSL コンポーネントを選択してインストールします。
- b. CA を PC のクライアントにダウンロードします。

構成ステップ

トムがマネージメント・セントラル・サーバーで SSL を使用可能にするためには、まずその前に前提条件のプログラムをインストールし、セントラル・システムにデジタル証明書をセットアップする必要があります。続きを行う前に、このシナリオに関する『前提条件および前提事項』を参照してください。前提条件を満たしたら、以下の手順を完了させて、マネージメント・セントラル・サーバーですべての接続を保護できます。

注: SSL が iSeries ナビゲーターで使用可能になっている場合、トムは SSL をマネージメント・セントラル・サーバーで使用可能にする前に、iSeries ナビゲーターでの SSL を使用不可にする必要があります。SSL が iSeries ナビゲーターで使用可能であり、マネージメント・セントラル・サーバーでは使用可能でない場合は、iSeries ナビゲーターがセントラル・システムと接続しようとしても、失敗します。

- ステップ 1: サーバー認証用にセントラル・システムを構成する
- ステップ 2: サーバー認証用にエンドポイント・システムを構成する
- ステップ 3: セントラル・システム上のマネージメント・セントラル・サーバーを再始動する
- ステップ 4: すべてのエンドポイント・システム上のマネージメント・セントラル・サーバーを再始動する
- ステップ 5: iSeries ナビゲーター・クライアントについて SSL をアクティブにする
- ステップ 6: クライアント認証用にセントラル・システムを構成する
- ステップ 7: クライアント認証用にエンドポイント・システムを構成する
- ステップ 8: 妥当性検査リストをエンドポイント・システムにコピーする
- ステップ 9: セントラル・システム上のマネージメント・セントラル・サーバーを再始動する
- ステップ 10: すべてのエンドポイント・システム上のマネージメント・セントラル・サーバーを再始動する

拡張した構成ステップを表示するには、『構成の詳細: SSL によるマネージメント・セントラル・サーバーへのすべての接続の保護』を参照してください。

構成の詳細: SSL によるマネージメント・セントラル・サーバーへのすべての接続の保護

次の情報は、『シナリオ: SSL によるマネージメント・セントラル・サーバーへのすべてのクライアント接続の保護』に目を通していただくことを前提としています。ここで、マネージメント・セントラル・サーバーに対するすべての接続をセキュアにするのに必要なステップを実行する方法を理解します。トムがシナリオを完了するのを追っていきます。

トムがマネージメント・セントラル・サーバーで SSL を使用可能にするためには、まずその前に前提条件のプログラムをインストールし、iSeries サーバーにデジタル証明書をセットアップする必要があります。続きを行う前に、このシナリオに関する『前提条件および前提事項』を参照してください。前提条件を満たしたら、以下の手順を完了させて、マネージメント・セントラル・サーバーですべての接続を保護できます。

注: iSeries ナビゲーターで SSL が使用可能になった場合、トムはマネージメント・セントラル・サーバーで SSL を使用可能にするために、iSeries ナビゲーターで SSL を使用不可にする必要があります。

SSL が iSeries ナビゲーターで使用可能であり、マネージメント・セントラル・サーバーでは使用可能でない場合は、iSeries ナビゲーターがセントラル・システムと接続しようとしても、失敗します。

ステップ 1: サーバー認証用にセントラル・システムを構成する

トムは SSL を使用することで、セントラル・システムとエンドポイント・システム間の伝送、および iSeries ナビゲーター・クライアントとセントラル・システム間の伝送をセキュアにすることができます。SSL では、証明書の移送と認証、およびデータの暗号化を行うことができます。SSL 接続が可能なのは、SSL が使用可能なセントラル・システムと SSL が使用可能なエンドポイント・システムの間だけです。トムは、クライアントの認証を構成する前に、サーバーの認証を構成する必要があります。

1. iSeries ナビゲーターで、「マネージメント・セントラル」を右クリックし、「プロパティ」を選択します。
2. 「セキュリティ」タブをクリックし、「Secure Sockets Layer (SSL) を使用する (Use Secure Sockets Layer (SSL))」を選択します。
3. 認証レベルとして「サーバー (Server)」を選択します。
4. 「OK」をクリックして、この値をセントラル・システムに設定します。

注: エンドポイント・システムのサーバー認証用の構成が完了するまで、マネージメント・セントラル・サーバーを再始動しないでください。

5. サーバー認証用にエンドポイント・システムを構成します。

ステップ 2: サーバー認証用にエンドポイント・システムを構成する

トムは、セントラル・システムでサーバー認証を構成した後に、すべてのエンドポイント・システムにサーバー認証を構成する必要があります。次のタスクを実行します。

1. 「マネージメント・セントラル」を展開する。
2. エンドポイント・システムのシステム値を比較および更新する。
 - a. 「エンドポイント・システム」において、セントラル・システムを右クリックし、「インベントリー」->「収集」の順に選択します。
 - b. セントラル・システムで使用しているシステム値のインベントリーを収集するために、「収集」ダイアログで「システム値」オプションをチェックします。他のオプションを選択解除します。
 - c. 「システム・グループ」->「新規システム・グループ」の順に右クリックします。
 - d. SSL を使用して接続するすべてのエンドポイント・システムを含む新規のシステム・グループを定義します。
 - e. 新規グループを表示するには、システム・グループのリストを展開します。
 - f. 収集が完了した後に、新規のシステム・グループを右クリックして、「システム値」->「比較および更新」と選択します。
 - g. 「モデル・システム」フィールドにセントラル・システムが表示されていることを確認します。
 - h. 「マネージメント・セントラル」カテゴリーを選択して以下の値を確認し、それぞれの隣にあるボックスをチェックします。
 - 「Secure Sockets Layer を使用する (Use Secure Sockets Layer (SSL))」で「Yes」を指定します。
 - SSL 認証レベルとして「サーバー (Server)」を指定します。

これらの値は、『サーバー認証用にセントラル・システムを構成する』の手順でセントラル・システムに設定します。

- i. 「**OK**」をクリックして、これらの値を新規のシステム・グループのエンドポイント・システムに設定します。
- j. 「**比較および更新**」が完了するのを待ってから、マネージメント・セントラル・サーバーを再始動します。これには、数分を要することがあります。

ステップ 3: セントラル・システム上のマネージメント・セントラル・サーバーを再始動する

1. iSeries ナビゲーターで、「**ユーザー接続**」を展開します。
2. 「セントラル・システム (central system)」ビューを展開します。
3. 「ネットワーク」->「サーバー」の順に展開し、「**TCP/IP**」を選択します。
4. 「マネージメント・セントラル」を右クリックし、「**停止**」を選択します。「セントラル・システム (central system)」ビューは縮小表示され、サーバーには接続されていないという内容のメッセージが表示されます。
5. マネージメント・セントラル・サーバーが停止したら、「**開始**」をクリックして、再始動します。

ステップ 4: すべてのエンドポイント・システム上のマネージメント・セントラル・サーバーを再始動する

1. 再始動するエンドポイント・システムを展開します。
2. 「ネットワーク」->「サーバー」の順に展開し、「**TCP/IP**」を選択します。
3. 「マネージメント・セントラル」を右クリックし、「**停止**」を選択します。
4. マネージメント・セントラル・サーバーが停止したら、「**開始**」をクリックして、再始動します。
5. それぞれのエンドポイント・システムについて、この手順を繰り返します。

ステップ 5: iSeries ナビゲーター・クライアントについて SSL をアクティブにする

1. iSeries ナビゲーターで、「**ユーザー接続**」を展開します。
2. セントラル・システムを右クリックし、「**プロパティ**」を選択します。
3. 「**セキュア・ソケット (Secure Sockets)**」タブをクリックし、「**接続に Secure Sockets Layer (SSL) を使用する (Use Secure Sockets Layer (SSL) for connection)**」を選択します。
4. iSeries ナビゲーターを終了し、再始動します。

ステップ 6: クライアント認証用にセントラル・システムを構成する

これで、トムはサーバー認証用の構成を終了したので、以下のオプションのクライアント認証手順を実行することができます。クライアント認証では、エンドポイント・システムとセントラル・システムの両方について、認証局とトラステッド・グループの妥当性検査を行います。セントラル・システム (SSL クライアント) が SSL を使用してエンドポイント・システム (SSL サーバー) に接続しようとした場合、セントラル・システムとエンドポイント・システムは、クライアント認証により互いの証明書を認証します。また、これは、認証局 (CA) とトラステッド・グループの認証と呼ばれます。

注: サーバーの認証を構成するまで、クライアントの認証の構成は完了できません。

1. iSeries ナビゲーターで、「**マネージメント・セントラル**」を右クリックし、「**プロパティ**」を選択します。
2. 「**セキュリティ (Security)**」タブをクリックし、「**Secure Sockets Layer (SSL) を使用する (Use Secure Sockets Layer (SSL))**」を選択します。
3. 認証レベルの「**クライアントおよびサーバー (Client and server)**」を選択します。
4. 「**OK**」をクリックして、この値をセントラル・システムに設定します。

注: すべてのエンドポイント・システムでクライアント認証およびサーバー認証に SSL を使用するよう構成し終えるまで、マネージメント・セントラル・サーバーを再始動しないでください。

5. クライアント認証用にエンドポイント・システムを構成します。

ステップ 7: クライアント認証用にエンドポイント・システムを構成する

1. エンドポイント・システムのシステム値を比較および更新する。

注: このタスクは、V4R5 を実行しているエンドポイントの iSeries サーバーでは正常に動作しません。

- a. 「エンドポイント・システム」において、セントラル・システムを右クリックし、「インベントリー」->「収集」の順に選択します。
- b. セントラル・システムで使用しているシステム値のインベントリーを収集するために、「収集」ダイアログで「システム値」オプションをチェックします。他のオプションを選択解除します。
- c. 「システム・グループ」->「新規システム・グループ」の順に右クリックします。
- d. SSL を使用して接続するすべてのエンドポイント・システムを含む新規のシステム・グループを定義します。
- e. 新規グループを表示するには、システム・グループのリストを展開します。
- f. 収集が完了した後に、新規のシステム・グループを右クリックして、「システム値」->「比較および更新」と選択します。
- g. 「モデル・システム」フィールドにセントラル・システムが表示されていることを確認します。
- h. 「マネージメント・セントラル」カテゴリを選択して以下の値を確認します。
 - 「Secure Sockets Layer を使用する (Use Secure Sockets Layer (SSL))」で「Yes」を指定します。
 - SSL 認証レベルとして「クライアントおよびサーバー (Client and Server)」を指定します。これらの値は、『クライアント認証用にセントラル・システムを構成する』の手順でセントラル・システムに設定します。それぞれの値の隣にある「更新」ボックスをチェックします。
- i. 「OK」をクリックして、これらの値を新規のシステム・グループのエンドポイント・システムに設定します。

ステップ 8: 妥当性検査リストをエンドポイント・システムにコピーする

1. 以下の手順は、ご使用のセントラル・システムが V5R3 以上であることを前提としています。iSeries ナビゲーターで、「マネージメント・セントラル」->「定義」の順に展開します。
2. 「パッケージ」を右クリックし、「新規定義 (New Definition)」を選択します。
3. 「新規定義 (New Definition)」ウィンドウで、以下のものについての作業を行います。
 - 名前: 定義名を入力する。
 - ソース・システム: セントラル・システム名を選択する。
 - 選択されているファイルとフォルダー: フィールド内をクリックし、/QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL と入力する。
4. 「オプション」タブをクリックし、「既存のファイルを送信されるファイルに置き換える (Replace existing file with the file being sent)」を選択します。
5. 「拡張 (Advanced)」をクリックします。
6. 「拡張オプション (Advanced Options)」ウィンドウで、「はい」を指定して、復元操作時にオブジェクトの違いが許されるようにします。
7. 「OK」をクリックして、定義のリストを最新表示し、新規のパッケージを表示します。

8. 新規パッケージを右クリックし、「送信」を選択します。
9. 「送信」ダイアログで、「使用可能なシステムとグループ (Available Systems and Groups)」リストから、「システム・グループ (System Groups) -> トラステッド・グループ (Trusted Group)」を展開します。V5R3 以上のシステムをすべて「選択されているシステムとグループ (Selected Systems and Group)」リストに個別に追加します。「選択されているシステムとグループ (Selected Systems and Group)」リストから他のすべてのシステムを除去し、「OK」をクリックします。トラステッド・グループは、『ステップ 7: クライアント認証用にエンドポイント・システムを構成する』の 1.c. で定義したシステム・グループです。

注: セントラル・システムは常にソース・システムであるため、「送信」タスクは、セントラル・システムでは常に失敗します。「送信」タスクは、すべてのエンドポイント・システムで正常に完了するはずですが。

V5R3 よりも前の iSeries システムでは、QYPSVLDL.VLDL は QMGTC2.LIB ではなく、QUSRSYS.LIB がありました。したがって、ご使用のシステムが V5R3 よりも前の場合、妥当性検査リストをそのシステムに送信して、QMGTC2.LIB ではなく QUSRSYS.LIB にセットする必要があります。これを行うには以下の手順を実行します。

- a. 上記で作成したパッケージ定義上で右クリックし、「新規ベース・オン (New Based On)」を選択します。
- b. 新規の名前を最初の定義と区別するための定義を行います。
- c. 定義の「一般 (General)」タブの「ターゲット・パス (Target Path)」列で、パス /QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL をクリックします。これでパスの編集ができます。QMGTC2 を QUSRSYS に変更します。

注: 「ソース・パス (Source Path)」ではなく「ターゲット・パス (Target Path)」を編集することを確認してください。

- d. 「OK」をクリックして新規パッケージ定義を保管します。
- e. 新規パッケージ定義を右クリックし、「送信」を選択します。
- f. 「送信」ダイアログで、「使用可能なシステムとグループ (Available Systems and Groups)」リストから、「システム・グループ (System Groups) -> トラステッド・グループ (Trusted Group)」を展開します。V5R3 よりも前のシステムをすべて「選択されているシステムとグループ (Selected Systems and Group)」リストに個別に追加します。「選択されているシステムとグループ (Selected Systems and Group)」リストから他のすべてのシステムを除去し、「OK」をクリックします。トラステッド・グループは、『ステップ 7: クライアント認証用にエンドポイント・システムを構成する』の 1.c. で定義したシステム・グループです。

ステップ 9: セントラル・システム上のマネージメント・セントラル・サーバーを再始動する

1. iSeries ナビゲーターで、「ユーザー接続」を展開します。
2. セントラル・システムを展開します。
3. 「ネットワーク」->「サーバー」の順に展開し、「TCP/IP」を選択します。
4. 「マネージメント・セントラル」を右クリックし、「停止」を選択します。「セントラル・システム (central system)」ビューは縮小表示され、サーバーには接続されていないという内容のメッセージが表示されます。
5. マネージメント・セントラル・サーバーが停止したら、「開始」をクリックして、再始動します。

ステップ 10: すべてのエンドポイント・システム上のマネージメント・セントラル・サーバーを再始動する

注: それぞれのエンドポイント・システムについて、この手順を繰り返します。

1. 再始動するエンドポイント・システムを展開します。
2. 「ネットワーク」->「サーバー」の順に展開し、「TCP/IP」を選択します。
3. 「マネージメント・セントラル」を右クリックし、「停止」を選択します。
4. マネージメント・セントラル・サーバーが停止したら、「開始」をクリックして、再始動します。

他の SSL のシナリオのリンクに関しては、『シナリオ』を参照してください。

概念

SSL プロトコルを使用することによって、クライアントとサーバー・アプリケーション間でセキュアな接続を確立して、通信セッションの一方のエンドポイントまたは両方のエンドポイントを認証できるようになります。SSL は、クライアントとサーバー・アプリケーション間でやり取りするデータのプライバシーと健全性も維持します。

以下の概念に関する情報は、SSL と iSeries サーバーとの間の関係をより良く理解するのに役立ちます。

- SSL の歴史
- SSL の機能
- サポートされている SSL および Transport Layer Security (TLS) プロトコル
- サーバー認証
- クライアント認証

SSL の歴史

Secure Sockets Layer (SSL) プロトコルは、インターネットのセキュリティについて関心が高まったことを受けて、1994 年に Netscape が開発しました。SSL は、当初は Web ブラウザーやサーバー通信をセキュアにするために開発されましたが、その仕様は TELNET や FTP などの他のアプリケーションも SSL を使用できるように作成されました。SSL および関連するプロトコルの詳細は、『サポートされている SSL および Transport Layer Security (TLS) プロトコル』を参照してください。

SSL の仕組み

SSL は、実際は 2 つのプロトコルからなっています。つまり、レコード・プロトコルとハンドシェイク・プロトコルです。レコード・プロトコルは、SSL セッションの 2 つのエンドポイント間のデータの流れを制御します。

ハンドシェイク・プロトコルは、SSL セッションの一方のエンドポイントまたは両方のエンドポイントを認証し、その SSL セッション用データの暗号化や暗号化解除に使用する鍵のセットを生成する固有な対称鍵を 1 つ設定します。SSL は、非対称暗号、デジタル証明書、および SSL ハンドシェイク・フローを使用して、SSL セッションの一方のエンドポイントまたは両方のエンドポイントを認証します。通常 SSL はサーバーを認証しますが、オプションでクライアントを認証します。認証局によって発行されるデジタル証明書は、各エンドポイントに割り当てられることも、または接続の各エンドポイントで SSL を使用するアプリケーションに割り当てられることもできます。

デジタル証明書は、公開鍵と、トラステッド認証局 (CA) がデジタル署名した識別情報からなっています。各公開鍵には、秘密鍵が 1 つずつ関連付けられています。秘密鍵は、証明書と一緒に、またはその一部として保管されることはありません。サーバー認証の場合もクライアント認証の場合も、認証されるエンドポイントは、デジタル証明書に含まれている公開鍵に関連付けられた秘密鍵にアクセスできることを証明しなければなりません。

SSL ハンドシェークは、公開鍵と秘密鍵を使用する暗号操作のために、パフォーマンス集約型の操作になってしまいます。2つのエンドポイント間で最初に SSL セッションが確立されたときに、これらの2つのエンドポイントとアプリケーションに関する SSL セッション情報をセキュアなメモリーにキャッシュすることで、後続の SSL セッションを迅速に使用可能にすることができます。SSL セッションが再開されると、2つのエンドポイントはハンドシェーク・フローを簡略化して、それぞれのエンドポイントが固有の情報に対するアクセス権を持っていることを、公開鍵や秘密鍵を使用することなく認証します。両方のエンドポイントがこの固有の情報にアクセスできることを証明できた場合は、次に、新しい対称鍵が設定され、SSL セッションが「再開」されます。TLS バージョン 1.0 と SSL バージョン 3.0 のセッションでは、キャッシュに入れられた情報が、24 時間を超えてセキュア・メモリーに残っていることはありません。V5R2M0 の場合は、暗号化ハードウェアを使用してメイン CPU に対する SSL ハンドシェークのパフォーマンスの影響を最小限にすることができます。

サポートされている SSL および Transport Layer Security (TLS) プロトコル

いくつかのバージョンの SSL プロトコルが定義されています。最新バージョンである Transport Layer Security (TLS) プロトコルは、SSL 3.0 に基づいており、Internet Engineering Task Force (IETF) が作成したものです。OS/400 インプリメンテーションは、以下のバージョンの SSL プロトコルおよび TLS プロトコルをサポートします。

- TLS バージョン 1.0
- TLS バージョン 1.0 (SSL バージョン 3.0 との互換性を持つもの)

注:

1. TLS バージョン 1.0 (SSL バージョン 3.0 との互換性を持つもの) では、まず、可能な場合は TLS が折衝され、この折衝が可能でない場合には次に、SSL バージョン 3.0 が折衝されます。SSL バージョン 3.0 が折衝できないと、SSL ハンドシェークは失敗します。
2. SSL バージョン 3.0 と SSL バージョン 2.0 間の互換性を持つ TLS バージョン 1.0 もサポートされます。これを指定するには、プロトコル値を「すべて」にします。つまり、可能な場合は TLS が折衝され、この折衝が可能でない場合には次に SSL バージョン 3.0 が折衝されます。SSL バージョン 3.0 が折衝できない場合は、SSL バージョン 2.0 が折衝されます。SSL バージョン 2.0 が折衝できないと、SSL ハンドシェークは失敗します。

- SSL バージョン 3.0
- SSL バージョン 2.0
- SSL バージョン 3.0 (SSL バージョン 2.0 との互換性を持つもの)


SSL バージョン 3.0 と SSL バージョン 2.0

SSL バージョン 3.0 は、SSL バージョン 2.0 とは大きく異なるプロトコルです。この両者の大きな違いは、以下のとおりです。

- SSL バージョン 3.0 のハンドシェーク・プロトコル・フローは、SSL バージョン 2.0 のフローと異なっています。
- SSL バージョン 3.0 は、RSA Data Security, Incorporated. 社の BSAFE 3.0 インプリメンテーションを使用しています。BSAFE 3.0 には、いくつかのタイミングの攻撃の修正と SHA-1 ハッシュ・アルゴリズムが組み込まれています。SHA-1 ハッシュ・アルゴリズムは、MD5 ハッシュ・アルゴリズムよりもセキュアであると考えられます。SHA-1 によって、MD5 の代わりに SHA-1 を使用する追加の暗号スイートを SSL バージョン 3.0 がサポートできるようになります。

- SSL バージョン 3.0 プロトコルは、SSL ハンドシェイク処理中に man-in-the-middle (MITM) (中継) アタックの発生を抑えます。SSL バージョン 2.0 では、まれに MITM アタックが暗号化仕様を弱めてしまう可能性がありました。暗号化が弱まると、無許可の人に SSL セッション鍵を壊す機会を与える可能性があります。

TLS バージョン 1.0 と SSL バージョン 3.0 の対比

SSL バージョン 3.0 を基にした Transport Layer Security (TLS) バージョン 1.0 は、最新の業界標準 SSL プロトコルです。その仕様は、Internet Engineering Task Force (IETF) により RFC 2246、『The TLS Protocol』 に定義されています。

TLS の主要な目標は、SSL をよりセキュアにし、このプロトコルの仕様をより正確かつ完全にすることです。TLS は、SSL バージョン 3.0 に対して以下のような拡張を行っています。

- よりセキュアな MAC アルゴリズム
- より細分化されたアラート
- 「グレー・エリア」仕様のより明確な定義

SSL が使用可能になっている iSeries サーバー・アプリケーションは、SSL バージョン 3.0 または SSL バージョン 2.0 のみを使用するよう別途要求しない限り、自動的に TLS によってサポートされます。

TLS では、以下のようなセキュリティーの改善を行っています。

- **Key-Hashing for Message Authentication**

TLS は、Key-Hashing for Message Authentication Code (HMAC (メッセージ確認コード用キー・ハッシュ)) を使用します。この機能は、レコードがインターネットのようなオープン・ネットワークを通過しているときに変更されないようにします。SSL バージョン 3.0 も鍵付きメッセージ認証を提供しますが、SSL バージョン 3.0 が使用する MAC (Message Authentication Code (メッセージ確認コード)) よりも、HMAC の方がよりセキュアです。

- **Enhanced Pseudorandom Function (PRF)**

PRF は、鍵データを生成します。TLS では、PRF は HMAC で定義されます。PRF は、そのセキュリティーを保証する 2 つのハッシュ・アルゴリズムを使用します。いずれかのアルゴリズムが露出した場合は、2 番目のアルゴリズムが露出しない限り、そのデータがセキュアな状態を持続します。

- **終了メッセージ検査の改善**

TLS バージョン 1.0 と SSL バージョン 3.0 はどちらも、交換されたメッセージが変更されなかったことを認証する終了メッセージを両方のエンドポイントに提供します。ただし、TLS の場合は、この終了メッセージは PRF 値および HMAC 値に基づいて作成されるので、SSL バージョン 3.0 よりもセキュアです。

- **一貫性のある証明書処理**

SSL バージョン 3.0 と異なり、TLS は、TLS インプリメンテーション間で交換する必要のある証明書のタイプを指定します。

- **特定のアラート・メッセージ**

TLS は、より具体的な内容の追加のアラートを提供して、いずれかのエンドポイントで検出された問題を指摘します。TLS は、特定のアラートをいつ送信するかについても文書化します。

サーバー認証

サーバー認証の場合、クライアントは、サーバー証明書が有効であり、このクライアントが信頼する認証局 (CA) によってそれが署名されていることを確認します。SSL は、非対称暗号およびハンドシェイク・プロトコル・フローを使用して、この固有な SSL セッションだけに使用する対称鍵を生成します。対称鍵は、

SSL セッションを流れるデータの暗号化と暗号化解除に使用する鍵のセットを生成するために使用します。次に、SSL ハンドシェイクが完了すると、通信リンクの一方のエンドポイントまたは両方のエンドポイントが認証されます。そして、データの暗号化と暗号化解除に使用する固有な鍵が生成されます。ハンドシェイクが完了すると、暗号化されたアプリケーション層データがその SSL セッションを流れます。

クライアント認証

多くのアプリケーションは、クライアント認証を使用可能にするオプションを備えています。クライアント認証の場合、サーバーは、クライアント証明書が有効で、かつサーバーが信頼する認証局によって署名されていることを確認します。以下の iSeries サーバーは、クライアント認証をサポートします。

- IBM HTTP Server (powered by Apache)
- FTP サーバー
- Telnet サーバー
- マネージメント・セントラル・エンドポイント・システム
- ディレクトリー・サービス (LDAP)

SSL を使用可能にする計画

iSeries サーバーで SSL を使用可能にすることを計画するときには、以下のことを考慮します。

- SSL の前提条件
- デジタル証明書のタイプおよび取得場所

SSL の前提条件

- IBM デジタル証明書マネージャー (DCM)、OS/400 のオプション 34 (5722-SS1)
- TCP/IP Connectivity Utilities for iSeries (5722-TC1)
- IBM HTTP Server for iSeries (5722-DG1)
- HTTP サーバーを使用して DCM を使用している場合には、IBM Developer Kit for Java™ (5722-JV1) をインストール済みであるか、または HTTP 管理サーバーが始動しないことを確認します。
- IBM Cryptographic Access Provider プロダクト (5722-AC3) (128 ビット)。このプロダクトのビット・サイズは、暗号操作で使用できる対称鍵内の秘密部分の最大サイズです。対称鍵に許されるサイズは、それぞれの国の輸出入関係法律によって規制されています。ビット・サイズが大きいと、よりセキュアな接続になります。
- 暗号化ハードウェアをインストールし、SSL で使用するように構成して、SSL ハンドシェイク処理の速度を高めることもできます。使用可能なオプションの詳細は、『暗号化ハードウェア』を参照してください。4758 IBM Cryptographic Coprocessor または 4764 IBM Cryptographic Coprocessor をインストールする場合は、オプション 35、暗号サービス・プロバイダーもインストールする必要があります。

iSeries Access for Windows コンポーネントで SSL を使用する場合は、iSeries Client Encryption プロダクト (5722-CE3) (128 ビット) もインストールする必要があります。iSeries Access for Windows では、セキュアな接続を確立するためにこの製品が必要です。

注: パーソナル・コミュニケーションズ・プロダクトに同梱されている PC5250 エミュレーターを使用する場合は、Client Encryption プロダクトをインストールする必要はありません。パーソナル・コミュニケーションズには独自の暗号コードが組み込まれています。

デジタル証明書

公衆デジタル証明書と専用デジタル証明書の違い、およびそれらを取得するためのオプションをより良く理解するには、『公衆証明書の使用と専用証明書の発行』を参照してください。

IBM デジタル証明書マネージャー (DCM) は、デジタル証明書管理のための iSeries サーバーのソリューションです。DCM の使用の詳細については、Information Center のトピック『デジタル証明書マネージャーの使用』を参照してください。

SSL によるアプリケーションの保護

以下の iSeries サーバー・アプリケーションは、SSL を使用することでセキュアにすることができます。

- エンタープライズ識別マッピング (EIM)
- FTP サーバー
- HTTP サーバー (Apache で稼動)
- iSeries Access for Windows
- ディレクトリー・サービス・サーバー (LDAP)
- 分散リレーショナル・データベース・アーキテクチャー (DRDA[®]) および分散データ管理 (DDM) サーバー
- マネージメント・セントラル・サーバー
- Telnet サーバー
- Websphere Application Server — Express
- iSeries Access for Windows の API (Application Programming Interface) セットに記述されているアプリケーション。
- iSeries サーバーでサポートされるセキュア・ソケットのアプリケーション・プログラミング・インターフェース (API) を使用して開発されるアプリケーション。サポートされる API は、グローバル・セキュア・ツールキット (GSKit) および SSL_iSeries のネイティブ API です。GSKit および SSL_API の詳細は、『Secure Sockets Layer (SSL) APIs』を参照してください。

SSL のトラブルシューティング

このきわめて基本的なトラブルシューティング情報は、SSL の使用中に iSeries サーバーが直面する可能性のある一連の問題を軽減することを目的としています。ただし、トラブルシューティングに関するすべての情報源ではなく、単に手引きである点にご注意ください。

以下の内容に当てはまることを確認します。

- iSeries サーバーで SSL の前提条件を満たしている (SSL の前提条件を参照)。
- V5R1 システムで iSeries ナビゲーターのマネージメント・セントラル・テクノロジーを使用している場合、以下の PTF をシステムにインストール済みである。
 - si01375
 - si01376
 - si01377
 - si01378
 - si01838
- 使用している認証局および証明書は有効であり、有効期限が切れていない。

前述の内容がご使用のシステムに当てはまることを確認しても、依然として SSL 関連の問題がある場合は、オプションで以下を試行してください。

- エラーに関する詳細については、サーバーのジョブ・ログにある SSL のエラー・コードをエラー・テーブルで相互参照することができます。セキュア・ソケットのエラー・コード・メッセージの情報にアクセスするには、『セキュア・ソケット API エラー・コード・メッセージ』ページを参照してください。たとえば、このテーブルではサーバーのジョブ・ログに示された -93 は、定数 `SSL_ERROR_SSL_NOT_AVAILABLE` にマップされます。
 - 負の戻りコード (コード番号の前にあるダッシュで表される) は、`SSL_API` を使用していることを表します。
 - 正の戻りコードは、`GSKit API` を使用していることを表します。プログラマーは、プログラム内で `gsk_strerror()` API または `SSL_strerror()` API をコーディングして、エラーの戻りコードの要旨を取得することができます。一部のアプリケーションはこの API を使用し、この文を含めたメッセージをジョブ・ログへ出力します。

詳細な情報が必要な場合は、このエラーについての考えられる原因および回復方法を示すために、テーブルに提供されているメッセージ ID を iSeries サーバー上に表示することができます。これらのエラー・コードに関するその他の説明は、エラーを戻した個々のセキュア・ソケット API 内で見つかる場合もあります。

- 以下の 2 つのヘッダー・ファイルには、テーブルに存在するものと同じシステム SSL の戻りコードの定数名が存在しますが、相互参照のためのメッセージ ID は存在しません。
 - `QSYSINC/H.GSKSSL`
 -



`QSYSINC/H.QSOSSL` ←

システム SSL の戻りコードの名前はこれらの 2 つのファイル内では変化しませんが、それぞれの戻りコードには複数の固有のエラーが関連する場合があります。

iSeries サーバーに関連するトラブルシューティングの詳細は、『トラブルシューティングとサービス』ページを参照してください。



関連情報

SSL の追加情報は、以下の情報源からも見つけることができます。


IBM の情報源

- 『SSL および Java Secure Socket Extension (JSSE)』ページには、JSSE およびその使用方法についての要旨が記載されています。
- 『IBM Toolbox for Java』ページには、使用可能な Java クラスおよびその使用方法についての要旨が記載されています。

Request For Comments (RFC)

- 『RFC 2246: The TLS Protocol Version 1.0』 では、TLS プロトコルについて詳細に説明しています。
- 『RFC2818: HTTP Over TLS』 では、TLS を使用してインターネットで HTTP 接続をセキュアにする方法について説明しています。

その他の情報源

- 『The SSL Protocol Version 3.0』文書  では、SSL プロトコル、バージョン 3.0 について詳細に説明しています。

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものであり、本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-0032
東京都港区六本木 3-2-31
IBM World Trade Asia Corporation
Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性があります。その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確認できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者をお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があります、単に目標を示しているものです。

商標

以下は、IBM Corporation の商標です。

DRDA
IBM
iSeries
Operating System/400
OS/400
Windows
Windows NT

Lotus[®]、Freelance、および WordPro は、IBM Corporation の商標です。

Microsoft[®]、Windows、Windows NT[®] および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

他の会社名、製品名およびサービス名などはそれぞれ各社の商標または登録商標です。

資料に関するご使用条件

お客様がダウンロードされる資料につきましては、以下の条件にお客様が同意されることを条件にその使用が認められます。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態を提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

これらの資料の著作権はすべて、IBM Corporation に帰属しています。

お客様が、このサイトから資料をダウンロードまたは印刷することにより、これらの条件に同意されたものとさせていただきます。



Printed in Japan